MISP Objects

MISP Objects

Generated from https://github.com/MISP/misp-objects.

MISP MISP objects to be used in MISP (2.4.80 (TBC)) system and can be used by other information sharing tool. MISP objects are in addition to MISP attributes to allow advanced combinations of attributes. The creation of these objects and their associated attributes are based on real cyber security use-cases and existing practices in information sharing.

ail-leak

An information leak as defined by the AIL Analysis Information Leak framework..

ail-leak is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
origin	url	The link where the leak is (or was) accessible at first-seen.	-
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✔
last-seen	datetime	When the leak has been accessible or seen for the last time.	✔
type	text	Type of information leak as discovered and classified by an AIL module.	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	A description of the leak which could include the potential victim(s) or description of the leak.	✔
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	-
first-seen	datetime	When the leak has been accessible or seen for the first time.	✔

cookie

An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser. The browser may store it and send it back with the next request to the same server. Typically, it's used to tell if two requests came from the same browser — keeping a user logged-in, for example. It remembers stateful information for the stateless HTTP protocol. (as defined by the Mozilla foundation..

cookie is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of cookie and how it's used in this specific object.	-
text	text	A description of the cookie.	✔
cookie-name	text	Name of the cookie (if splitted)	-
cookie	cookie	Full cookie	-
cookie-value	text	Value of the cookie (if splitted)	-

credit-card

A payment card like credit card, debit card or any similar cards which can be used for financial transactions..

credit-card is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
card-security-code	text	Card security code as embossed or printed on the card.	-
issued	datetime	Initial date of validity or issued date.	-
cc-number	cc-number	credit-card number as encoded on the card.	-
version	comment	yabin.py and regex.txt version used for the generation of the yara rules.	-
comment	comment	A description of the card.	-
name	text	Name of the card owner.	-
expiration	datetime	Maximum date of validity	-

ddos

DDoS object describes a current DDoS activity from a specific or/and to a specific target. Type of DDoS can be attached to the object as a taxonomy.

ddos is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
ip-src	ip-src	IP address originating the attack	-
dst-port	port	Destination port of the attack	-
ip-dst	ip-dst	Destination ID (victim)	-
total-pps	counter	Packets per second	-
total-bps	counter	Bits per second	-
last-seen	datetime	End of the attack	-
src-port	port	Port originating the attack	-
text	text	Description of the DDoS	-
protocol	text	Protocol used for the attack	-
first-seen	datetime	Beginning of the attack	-

domain|ip

A domain and IP address seen as a tuple in a specific time frame..

domain|ip is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
domain	domain	Domain name	-
text	text	A description of the tuple	-
last-seen	datetime	Last time the tuple has been seen	-

Object attribute	MISP attribute type	Description	Disable correlation
ip	ip-dst	IP Address	-
first-seen	datetime	First time the tuple has been seen	-

elf

Object describing a Executable and Linkable Format.

elf is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
entrypoint-address	text	Address of the entry point	✔
type	text	Type of ELF	-
arch	text	Architecture of the ELF file	-
text	text	Free text value to attach to the ELF	✔
number-sections	counter	Number of sections	✔
os_abi	text	Header operating system application binary interface (ABI)	-

elf-section

Object describing a section of an Executable and Linkable Format.

elf-section is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
text	text	Free text value to attach to the section	✔
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
name	text	Name of the section	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
flag	text	Flag of the section	✔
md5	md5	[Insecure] MD5 hash (128 bits)	-
type	text	Type of the section	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
entropy	float	Entropy of the whole section	✔

email

Email object describing an email with meta-information.

email is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
mime-boundary	email-mime-boundary	MIME Boundary	-
thread-index	email-thread-index	Identifies a particular conversation thread	-
header	email-header	Full headers	-
to	email-dst	Destination email address	-
from-display-name	email-src-display-name	Display name of the sender	-
from	email-src	Sender email address	-
attachment	email-attachment	Attachment	-
message-id	email-message-id	Message ID	-
reply-to	email-reply-to	Email address the reply will be sent to	-
subject	email-subject	Subject	-
send-date	datetime	Date the email has been sent	✔
to-display-name	email-dst-display-name	Display name of the receiver	-
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	-

file

File object describing a file with meta-information.

file is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	-
text	text	Free text value to attach to the file	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
mimetype	text	Mime type	✔
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔
authentihash	authentihash	Authenticode executable signature hash	-
md5	md5	[Insecure] MD5 hash (128 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
pattern-in-file	pattern-in-file	Pattern that can be found in the file	-
filename	filename	Filename on disk	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
entropy	float	Entropy of the whole file	✔
malware-sample	malware-sample	The file itself (binary)	-

geolocation

An object to describe a geographic location..

geolocation is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
region	text	Region.	-
city	text	City.	-
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔
last-seen	datetime	When the location was seen for the last time.	✔
country	text	Country.	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	A generic description of the location.	✔
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✔
altitude	float	The altitude is the decimal value of the altitude in the World Geodetic System 84 (WGS84) reference.	-
first-seen	datetime	When the location was seen for the first time.	✔

http-request

A single HTTP request header.

http-request is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
basicauth-password	text	HTTP Basic Authentication Password	-
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✔
cookie	text	An HTTP cookie previously sent by the server with Set-Cookie	-
text	text	HTTP Request comment	✔

Object attribute	MISP attribute type	Description	Disable correlation
proxy-user	text	HTTP Proxy Username	-
uri	uri	Request URI	-
user-agent	user-agent	The user agent string of the user agent	-
basicauth-user	text	HTTP Basic Authentication Username	-
host	hostname	The domain name of the server	-
content-type	other	The MIME type of the body of the request	-
proxy-password	text	HTTP Proxy Password	-
referer	referer	This is the address of the previous web page from which a link to the currently requested page was followed	-
url	url	Full HTTP Request URL	-

ip|port

An IP address and a port seen as a tuple (or as a triple) in a specific time frame..

ip|port is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
dst-port	port	Destination port	-
src-port	port	Source port	-
ip	ip-dst	IP Address	-

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	Last time the tuple has been seen	-
text	text	Description of the tuple	-
first-seen	datetime	First time the tuple has been seen	-

macho

Object describing a file in Mach-O format..

macho is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
entrypoint-address	text	Address of the entry point	✔
text	text	Free text value to attach to the Mach-O file	✔
number-sections	counter	Number of sections	✔
type	text	Type of Mach-O	-
name	text	Binary's name	-

macho-section

Object describing a section of a file in Mach-O format..

macho-section is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
text	text	Free text value to attach to the section	✔
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
name	text	Name of the section	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
md5	md5	[Insecure] MD5 hash (128 bits)	-
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
entropy	float	Entropy of the whole section	✔

passive-dns

Passive DNS records as expressed in draft-dulaunoy-dnsop-passive-dns-cof-01.

passive-dns is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
origin	text	Origin of the Passive DNS response	-
zone_time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	-
zone_time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	-
sensor_id	text	Sensor information where the record was seen	-
count	counter	How many authoritative DNS answers were received at the Passive DNS Server's collectors with exactly the given set of values as answers	-
text	text	-	-
rdata	text	Resource records of the queried resource	-
bailiwick	text	Best estimate of the apex of the zone where this data is authoritative	-
rrtype	text	Resource Record type as seen by the passive DNS	-

Object attribute	MISP attribute type	Description	Disable correlation
time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) has been seen by the passive DNS	-
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	-
rrname	text	Resource Record name of the queried resource	-

pe

Object describing a Portable Executable.

pe is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	-
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	-
legal-copyright	text	LegalCopyright in the resources	✔
company-name	text	CompanyName in the resources	✔
imphash	imphash	Hash (md5) calculated from the import table	-
text	text	Free text value to attach to the PE	✔

Object attribute	MISP attribute type	Description	Disable correlation
number-sections	counter	Number of sections	✔
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/	-
original-filename	filename	OriginalFilename in the resources	-
entrypoint-address	text	Address of the entry point	✔
lang-id	text	Lang ID in the resources	✔
type	text	Type of PE	✔
file-version	text	FileVersion in the resources	✔
product-name	text	ProductName in the resources	✔
product-version	text	ProductVersion in the resources	✔
file-description	text	FileDescription in the resources	✔
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✔
internal-filename	filename	InternalFilename in the resources	-

pe-section

Object describing a section of a Portable Executable.

pe-section is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
text	text	Free text value to attach to the section	✔
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
name	text	Name of the section	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
md5	md5	[Insecure] MD5 hash (128 bits)	-
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-

Object attribute	MISP attribute type	Description	Disable correlation
characteristic	text	Characteristic of the section	-
entropy	float	Entropy of the whole section	✔

person

An person which describes a person or an identity..

person is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
middle-name	middle-name	Middle name of a natural person	-
gender	gender	The gender of a natural person.	-
first-name	first-name	First name of a natural person.	-
passport-expiration	passport-expiration	The expiration date of a passport.	-
place-of-birth	place-of-birth	Place of birth of a natural person.	-
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	-
passport-number	passport-number	The passport number of a natural person.	-
nationality	nationality	The nationality of a natural person.	-
passport-country	passport-country	The country in which the passport was issued.	-

Object attribute	MISP attribute type	Description	Disable correlation
redress-number	redress-number	The Redress Control Number is the record identifier for people who apply for redress through the DHS Travel Redress Inquiry Program (DHS TRIP). DHS TRIP is for travelers who have been repeatedly identified for additional screening and who want to file an inquiry to have erroneous information corrected in DHS systems.	-
last-name	last-name	Last name of a natural person.	-
text	text	A description of the person or identity.	✔

phone

A phone or mobile phone object which describe a phone..

phone is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
serial-number	text	Serial Number.	-
text	text	A description of the phone.	✔
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	-

Object attribute	MISP attribute type	Description	Disable correlation
msisdn	text	MSISDN (pronounced as /'em es ai es di en/ or misden) is a number uniquely identifying a subscription in a GSM or a UMTS mobile network. Simply put, it is the mapping of the telephone number to the SIM card in a mobile/cellular phone. This abbreviation has a several interpretations, the most common one being Mobile Station International Subscriber Directory Number.	-
first-seen	datetime	When the phone has been accessible or seen for the first time.	✔
guti	text	Globally Unique Temporary UE Identity (GUTI) is a temporary identification to not reveal the phone (user equipment in 3GPP jargon) composed of GUMMEI and the M-TMSI.	-
imsi	text	A usually unique International Mobile Subscriber Identity (IMSI) is allocated to each mobile subscriber in the GSM/UMTS/EPS system. IMSI can also refer to International Mobile Station Identity in the ITU nomenclature.	-

Object attribute	MISP attribute type	Description	Disable correlation
imei	text	International Mobile Equipment Identity (IMEI) is a number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones.	-
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	-
last-seen	datetime	When the phone has been accessible or seen for the last time.	✔

r2graphity

Indicators extracted from files using radare2 and graphml.

r2graphity is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
callback-average	counter	Average size of a callback	✔
local-references	counter	Amount of API calls inside a code section	✔
total-api	counter	Total amount of API calls	✔
text	text	Description of the r2graphity object	✔
gml	attachment	Graph export in G>raph Modelling Language format	✔

Object attribute	MISP attribute type	Description	Disable correlation
total-functions	counter	Total amount of functions in the file.	✔
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✔
referenced-strings	counter	Amount of referenced strings	✔
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✔
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✔
callback-largest	counter	Largest callback	✔
create-thread	counter	Amount of calls to CreateThread	✔
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✔
not-referenced-strings	counter	Amount of not referenced strings	✔
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✔
r2-commit-version	text	Radare2 commit ID used to generate this object	✔
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✔

Object attribute	MISP attribute type	Description	Disable correlation
get-proc-address	counter	Amount of calls to GetProcAddress	✔
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✔
dangling-strings	counter	Amount of dangling strings (string with a code cross reference, that is not within a function. Radare2 failed to detect that function.)	✔
callbacks	counter	Amount of callbacks (functions started as thread)	✔
memory-allocations	counter	Amount of memory allocations	✔

regexp

An object describing a regular expression (regex or regexp). The object can be linked via a relationship to other attributes or objects to describe how it can be represented as a regular expression..

regexp is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
regexp	text	regexp	-
comment	comment	A description of the regular expression.	-
regexp-type	text	Type of the regular expression syntax.	✔

registry-key

Registry key object describing a Windows registry key with value and last-modified timestamp.

registry-key is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
data-type	reg-datatype	Registry value type	-
hive	reg-hive	Hive used to store the registry key (file on disk)	-
key	reg-key	Full key path	-
last-modified	datetime	Last time the registry key has been modified	-
name	reg-name	Name of the registry key	-
data	reg-data	Data stored in the registry key	-

tor-node

Tor node (which protects your privacy on the internet by hiding the connection between users Internet address and the services used by the users) description which are part of the Tor network at a time..

tor-node is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✔

Object attribute	MISP attribute type	Description	Disable correlation
version	text	parsed version of tor, this is None if the relay's using a new versioning scheme.	-
published	datetime	router's publication time. This can be different from first-seen and last-seen.	✔
version_line	text	versioning information reported by the node.	-
text	text	Tor node comment.	✔
address	ip-src	IP address of the Tor node seen.	-
document	text	Raw document from the consensus.	✔
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✔
description	text	Tor node description.	✔
flags	text	list of flag associated with the node.	-
nickname	text	router's nickname.	-
fingerprint	text	router's fingerprint.	-

url

url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata..

url is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
host	hostname	Full hostname	-
domain	domain	Full domain	-
last-seen	datetime	Last time this URL has been seen	-
text	text	Description of the URL	-
subdomain	text	Subdomain	-
fragment	text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	-
url	url	Full URL	-
credential	text	Credential (username, password)	-
tld	text	Top-Level Domain	-
first-seen	datetime	First time this URL has been seen	-
scheme	text	Scheme	-
query_string	text	Query (after path, preceded by '?')	-
port	port	Port number	-
resource_path	text	Path (between hostname:port and query)	-
domain_without_tld	text	Domain without Top-Level Domain	-

vulnerability

Vulnerability object describing common vulnerability enumeration.

vulnerability is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
modified	datetime	Last modification date	-
published	datetime	Initial publication date	-
vulnerable_configuration	text	The vulnerable configuration is described in CPE format	-
summary	text	Summary of the vulnerability	-
text	text	Description of the vulnerability	-
references	link	External references	-
id	vulnerability	Vulnerability ID (generally CVE, but not necessarely)	-

whois

Whois records information for a domain name..

whois is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
registar	whois-registar	Registar of the whois entry	-
text	text	Full whois entry	-

Object attribute	MISP attribute type	Description	Disable correlation
modification-date	datetime	Last update of the whois entry	-
registrant-name	whois-registrant-name	Registrant name	-
registrant-phone	whois-registrant-phone	Registrant phone number	-
expiration-date	datetime	Expiration of the whois entry	-
registrant-email	whois-registrant-email	Registrant email address	-
creation-date	datetime	Initial creation of the whois entry	-
domain	domain	Domain of the whois entry	-

x509

x509 object describing a X.509 certificate.

x509 is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
serial-number	text	Serial number of the certificate	-
issuer	text	Issuer of the certificate	-
validity-not-after	datetime	Certificate invalid after that date	-
validity-not-before	datetime	Certificate invalid before that date	-
version	text	Version of the certificate	-

Object attribute	MISP attribute type	Description	Disable correlation
x509-fingerprint-sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
text	text	Free text description of hte certificate	-
pubkey-info-modulus	text	Modulus of the public key	-
pubkey-info-size	text	Length of the public key (in bits)	-
x509-fingerprint-sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
raw-base64	text	Raw certificate base64 encoded	-
x509-fingerprint-md5	md5	[Insecure] MD5 hash (128 bits)	-
subject	text	Subject of the certificate	-
pubkey-info-exponent	text	Exponent of the public key	-
pubkey-info-algorithm	text	Algorithm of the public key	-

yabin

yabin.py generates Yara rules from function prologs, for matching and hunting binaries. ref: https://github.com/AlienVault-OTX/yabin.

yabin is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
whitelist	comment	Whitelist name used to generate the rules.	-

Object attribute	MISP attribute type	Description	Disable correlation
yara	yara	Yara rule generated from -y.	✔
comment	comment	A description of Yara rule generated.	-
yara-hunt	yara	Wide yara rule generated from -yh.	✔
version	comment	yabin.py and regex.txt version used for the generation of the yara rules.	-

Relationships

Default type of relationships in MISP objects.

Relationships are part of MISP object and available in JSON format at this location. The JSON format can be freely reused in your application or automatically enabled in MISP.

Name of relationship	Description	Format
derived-from	The information in the target object is based on information from the source object.	['misp', 'stix-2.0']
duplicate-of	The referenced source and target objects are semantically duplicates of each other.	['misp', 'stix-2.0']
related-to	The referenced source is related to the target object.	['misp', 'stix-2.0']
attributed-to	This referenced source is attributed to the target object.	['misp', 'stix-2.0']
targets	This relationship describes that the source object targets the target object.	['misp', 'stix-2.0']
uses	This relationship describes the use by the source object of the target object.	['misp', 'stix-2.0']
indicates	This relationships describes that the source object indicates the target object.	['misp', 'stix-2.0']

Name of relationship	Description	Format
mitigates	This relationship describes a source object which mitigates the target object.	['misp', 'stix-2.0']
variant-of	This relationship describes a source object which is a variant of the target object	['misp', 'stix-2.0']
impersonates	This relationship describe a source object which impersonates the target object	['misp', 'stix-2.0']
authored-by	This relationship describes the author of a specific object.	['misp']
located	This relationship describes the location (of any type) of a specific object.	['misp']
included-in	This relationship describes an object included in another object.	['misp']
analysed-with	This relationship describes an object analysed by another object.	['misp']
claimed-by	This relationship describes an object claimed by another object.	['misp']
communicates-with	This relationship describes an object communicating with another object.	['misp']
dropped-by	This relationship describes an object dropped by another object.	['misp']
executed-by	This relationship describes an object executed by another object.	['misp']
affects	This relationship describes an object affected by another object.	['misp']
beacons-to	This relationship describes an object beaconing to another object.	['misp']
abuses	This relationship describes an object which abuses another object.	['misp']
exfiltrates-to	This relationship describes an object exfiltrating to another object.	['misp']

Name of relationship	Description	Format
identifies	This relationship describes an object which identifies another object.	['misp']
intercepts	This relationship describes an object which intercepts another object.	['misp']
calls	This relationship describes an object which calls another objects.	['misp']
detected-as	This relationship describes an object which is detected as another object.	['misp']
triggers	This relationship describes an object which triggers another object.	['misp']